

Cybercrime: Italia terza al mondo per numero di attacchi

L'Italia si conferma uno dei Paesi al mondo più colpiti dal cybercrime. Malware, ransomware e phishing sono le minacce più temibili e le aziende sono il bersaglio preferito delle estorsioni, soprattutto le PMI dei settori dei servizi, sanità e finanziari.



Lo sostiene il report **"Stepping ahead of risk"**, di **Trend Micro Research** sulle minacce informatiche che hanno colpito nel corso del primo semestre 2023. L'Italia è il terzo Paese al mondo e il primo in Europa maggiormente colpito dai malware. In tutto il mondo, Trend Micro ha bloccato nella prima metà del 2023 un totale di oltre 85,6 miliardi di minacce, di cui circa 37 miliardi sono arrivate via mail.

Secondo l'ultimo report "Threatland" di Swascan, nel secondo trimestre 2023, il fenomeno del furto di dati sensibili con richiesta di riscatto è cresciuto del +34,6% in Italia e del +62% a livello globale rispetto al trimestre precedente. In Italia, l'80% delle vittime colpite sono pmi e il 91% sono aziende con fatturato inferiore ai 250 milioni di euro. Tra aprile e giugno scorsi in Italia si sono registrati numerosi attacchi informatici che hanno coinvolto soprattutto aziende di servizi (54%), del manifatturiero (11%) e dal sanitario (9%), più che raddoppiato rispetto al trimestre precedente. Circa 190mila i dispositivi compromessi nel nostro paese.

Secondo Trend Micro, l'Italia è al primo posto in Europa e al terzo su scala globale per attacchi malware, con un totale di 174.608.112 malware intercettati. Queste le prime cinque posizioni: Stati Uniti (417.545.421), Giappone (355.248.073), Italia (174.608.112), India (120.426.491), Brasile (96.908.591).

Per il micro-malware, l'Italia è il quarto Paese al mondo più colpito, con 5.180 attacchi. Sul podio Giappone (28.816), Stati Uniti (10.485) e Turchia (5.529).

Sempre secondo Trend Micro, le minacce via e-mail che hanno colpito l'Italia nel primo semestre 2023 sono state 048.776. Le visite ai siti malevoli sono state 470.479. I siti malevoli ospitati in Italia e bloccati sono stati 68.334. Il numero di app malevole scaricate nel primo semestre 2023 è di 724.698. Infine, i malware unici di online banking intercettati sono stati 804.

L'AI generativa nel cybercrime

L'espansione di strumenti di intelligenza artificiale generativa ha permesso ai cybercriminali di utilizzare nuovi tools come WormGpt e FraudGpt e di organizzare nuove truffe, come ad esempio i rapimenti virtuali, secondo Trend Micro.

L'uso dell'intelligenza artificiale consente ai cybercriminali di eseguire attacchi più elaborati e pone una nuova serie di sfide.

Ransomware, cresce la minaccia

Stando ai dati raccolti da Swascan per il secondo trimestre del 2023, sono state 1451 le vittime (colpite e soggette a pubblicazione di dati rubati) a livello globale di attacchi ransomware, caratterizzati dalla diffusione di software malevoli che criptano dati per il cui ripristino si chiede il pagamento di un riscatto. Si registra anche un incremento delle gang di cybercriminali dietro questi attacchi, passate da 36 a 43 (+19,4%). Lockbit si distingue come la più attiva, avendo orchestrato ben 245 attacchi nel corso del trimestre.

Questi attacchi sembrano avere un obiettivo preciso, le aziende. In particolare, quelle statunitensi sono state le più bersagliate, con 636 attacchi, seguite da quelle del Regno Unito (69) e del Canada (60). In Italia l'80% di questi ha colpito le pmi, dimostrando come i cybercriminali le ritengono più vulnerabili rispetto alle grandi aziende. Il 91% delle aziende italiane vittime ha un fatturato al di sotto dei 250 milioni di euro.

Anche la geografia del fenomeno si sta espandendo: mentre nel primo trimestre del 2023 erano 79 i Paesi colpiti, nel secondo sono diventati 89. Dall'inizio dell'anno, sono stati registrati complessivamente 2.349 attacchi, con un picco di attività a maggio dove sono avvenuti il 25% (575) degli attacchi totali.

Le aziende di servizi sono state le più colpite, rappresentando il 47% degli attacchi, seguite da quelle del settore manifatturiero (16%) e tecnologico (6%). Anche in Italia, il settore dei servizi è in cima alla lista con il 54% degli attacchi, seguito dal manifatturiero (11%) e dal sanitario (9%), più che raddoppiato rispetto al trimestre precedente. Tuttavia, la minaccia non ha risparmiato altri settori, tra cui il finanziario, il manifatturiero, l'immobiliare, e molti altri.

La minaccia emergente più diffusa è il phishing, con quasi 160.000 campagne rilevate. In Italia, le campagne di phishing hanno interessato principalmente il settore bancario, decisamente quello maggiormente preso di mira dagli attaccanti con lo scopo di esfiltrare credenziali di accesso ed informazioni di pagamento.

Furto e vendita di credenziali

L'analisi dei due principali marketplace di credenziali rubate condotta da Swascan ha portato alla luce come, solo nel secondo trimestre 2023, quasi 8 milioni di dispositivi (esattamente 7.756.466) siano stati compromessi su scala globale. Da questi dispositivi sono state "esfiltrate" credenziali preziose rendendo accessibili dati sensibili e informazioni personali. L'Italia non è stata risparmiata: sono 189.042 i dispositivi compromessi, pari al 2,4% del totale globale. A livello europeo, la cifra sale a 1.370.950 dispositivi, ovvero il 17,7%.

Swascan conferma che il malware rimangono una delle principali preoccupazioni per gli esperti di sicurezza e gli utenti. Da aprile a giugno di quest'anno gli "infostealer" – malware specializzati nel rubare informazioni confidenziali dagli host infettati – si sono distinti come la famiglia di malware più diffusa, consolidando il loro ruolo predominante nel mondo del cybercrime.